Agenda Item #:

ITEM TYPE: Discussion

BOARD AGENDA ITEM

TITLE: Proposed Policy EH: Data Governance

DATE: July 10, 2019

OVERVIEW: In light of the demonstrated need for the development of a Data Governance policy, staff is presenting background information, a draft policy, and draft administrative regulations for Board discussion.

The background information includes a brief analysis of system impact, connections to current policies, and relevant legal references. The information also provides several options for the implementation of the new policy as well as the staff recommendation.

LINK TO STRATEGIC PLAN:

Pillar II: Strengthen Productive Family and Community Partnerships

OBJECTIVE II.i: Communication between CCPS and the community demonstrates transparency, trust, and respect.

Pillar III: Develop and Support a Successful Workforce

OBJECTIVE III.ii: CCPS provides professional and leadership development to retain and promote an effective and culturally competent workforce.

Pillar IV: Establish Safe, Secure, Healthy and Modern Learning Environments

OBJECTIVE IV.iv: CCPS provides safe and secure schools, facilities, and assets that serve our students and communities.

FISCAL IMPACT: None

RECOMMENDATION/FUTURE DIRECTION: Staff request input on the proposed policy and approval to seek public input over the course of the next 30 days.

Submitted by:

Gregory Bricca, Chief of Strategic Planning and System Performance

Approve/Concur:

_____
Jason Anderson, Chief of Academics, Equity, and Accountability

_____
Steven A. Lockard, Ph.D., Superintendent of Schools

Proposed Board Policy EH – Data Governance
Background Information and Analysis

STATEMENT OF ISSUE

While the Board of Education of Carroll County has numerous policies that address topics related to Data Governance, the Board does not have policy that provides comprehensive expectations regarding system-wide data and information management.

BACKGROUND

During the 2018 Legislative Session, the Maryland General Assembly passed House Bill 568 – Student Data Governance. With the Governor's approval, the bill has been codified as §§ 7-2101 to 7-2105 under Subtitle 21 of the Education Article of Maryland Code. The statute requires the Maryland State Department of Education (MSDE), in consultation with the Maryland Department of Information Technology (DoIT) and the county boards of education to develop and update best practices for county boards on data governance policies and procedures.

In December 2018, the State Superintendent of Schools requested each County Board identify a Data Governance Designee to participate in state-wide meetings to identify and develop best practices. While the MSDE led process is ongoing, the group has provided numerous best practice documents from a variety of state and national sources.

Additionally, on April 16, 2019, the Office of Compliance and Monitoring (OCM) from MSDE conducted a compliance review of the Carroll County Public Schools (CCPS) internal controls over graduation rate reporting as well as the assessment of operational and programmatic controls and compliance with applicable laws, regulations, policies, and procedures. Based on findings from the monitoring, OCM has recommended that CCPS develop written policies and procedures for data management to ensure accuracy and that CCPS identify a data management team and data stewards related to grading and graduation related data.

While the need to establish written policy and procedure related to specific student data is clear, the need to establish written policy and procedure related to all CCPS data is no less important. For example, best practices in the fields of Human Resources and Financial Management also point to the need for documented data governance programs.

Data are ubiquitous throughout the school system; a documented, comprehensive, system-wide approach to Data Governance is a necessity.

In April 2019, Superintendent Lockard approved the Committee Charter for a Data Policy Committee (DPC) charged with creating the CCPS Data Governance Policy and Regulations. The DPC consists of the following members: Jason Anderson, Chantress Baptist, Gregg Bricca, Gary Davis, Chris Hartlove, Cindy McCabe and Karl Streaker.

The DCP reviewed the best practice documents provided by MSDE as well as Data Governance policies from other Maryland school systems. The DPC review examine several options and structures for the implantation of the CCPS Data Governance Program.

Proposed Board Policy EH – Data Governance
Background Information and Analysis

Ultimately, a fully matured Data Governance Program will impact all aspects of the school system. Once developed, at minimum, the program will include:

- A data privacy and security incident response plan;
- A breach notification plan;
- Procedures and requirements for permitting access to data;
- Guidelines for CCPS Data Stewards;
- Requirements for annually publishing information on:
    - Types of student data and personally identifiable information processed by the county board, the protocols for processing student data, and the rationales for selecting processing protocols;
    - Contracted services that involve sharing student data between a county board and a school service contract provider; and
    - Procedures and rationales for vetting and selecting Internet sites, services, and applications.
- Professional development on privacy and data security for all employees

The proposed policy will work in conjunction with numerous, pre-existing Board Policies and Administrative Regulations. The associated policies include:

- AF - Student Data Privacy Policy
- EHB - Data Records Retention
- IIAA Selection, Evaluation, and Adoption of Instructional Materials.
- IJND - Telecommunications Policy
- ILB - Test Security and Data Reporting
- JR - Disclosure of Directory Information
- JRB - Protection of Pupil Rights-Surveys, Physical Exams, Marketing Personal Information, and Inspection of Certain Material
- JRC - Family Educational Rights

The following legal documents will be used to guide the development of the CCPS Data Governance Plan reference in the proposed policy:

- Every Student Succeeds Act (ESSA), (20 U.S.C. §6301);
- The Family Educational Rights and Privacy Act (20 U.S.C. § 1232G; 34 C.F.R. § 99);
- Privacy Act of 1974 (5 U.S.C. § 552a)
- Maryland Personal Information Protection Act (Md. Code Com. Law Code §§ 14-3501 to -3508)
- Student Work Product – Claim of Copyright Prohibited (Md. Code Education § 4-130);
- Student Data Privacy Act of 2015 (Md. Code Education § 4-131);
- Student Data Governance (Md. Code Education §§ 7-2101 to -2105)
- Disposition of Records and Other Materials (Md. Code State Govt. §§ 10-614 to -619);
- Protection of Information by Government Agencies (Md. Code State Govt. §§ 10-1301 to -1308);
- COMAR 13A.08.02. Student Records;
- Maryland State Department of Education, “The Maryland Student Record Manual”;
- Maryland State Department of Education, “Records Retention and Disposition: A Reference Manual for Public Education in Maryland 2005”;

- Maryland Department of Information Technology, "Information Security Policy";
- Maryland Department of Legislative Services, Office Legislative Audits – Local School System Audit Standards.

The fiscal resources required to implement this policy will primarily be limited to staff time. Because of the scope of developing a comprehensive Data Governance Program, it is expected that it will require a significant commitment from administrative staff.

OPTIONS FOR IMPLEMENTATION

The DPC is providing a proposed policy and administrative regulations following the current practice of having the policy provide broad guidance on the issue and using the administrative regulation to set the directive for implementation. The current structure outlined in the proposed administrative regulations follows guidance and best practice documents provided by the United States Department of Education's Privacy Technical Assistance Center (PTAC) document "Data Governance and Stewardship: Privacy Technical Assistance Center Issue Brief " and the Statewide Longitudinal Data Systems (SLDS) Grant Program Technical Assistance document, "Single-Agency Data Governance: Roles and Responsibilities."

Several additional options for implementation exist. First, the Board could provide more specific guidance at the policy level. Best Practice documents suggest that the policy should provide a clear framework for system workgroups as they develop more detailed plans for the full implementation of the program.

Additionally, the Board could choose to delay implementation of the policy. MSDE has provided numerous resources regarding data governance policy and program development. However, the MSDE and DoIT work is ongoing. By delaying action on a policy, CCPS may receive additional guidance that could redirect the systems approach to data governance.

RECOMMENDATION

The DPC is recommending issuing a policy and administrative regulations following the current practice. Proceeding in this manner will enable the system to establish the groundwork for a Data Governance Program that will be flexible enough to adopt any new recommendations or best practices developed by MSDE and DoIT according to statutory requirements. Additionally, it will enable staff to begin the comprehensive task without further delay.

Building the Future CCPS Carroll County Public Schools	**Data Governance**	**Policy #**	EH
		Implemented	
		Reviewed/Updated	
Page 1 of 2			
Procedure Owner		**Expiration/Review**	

Policy

1. Purpose

To formalize an organizational approach to data and information management that encompasses the full lifecycle of school system data, from acquisition, to use, to disposal.

2. Definitions

The words used in this policy shall have their normal accepted meanings except as set forth below.

Data – quantitative or qualitative facts, figures, records, or information related to students, staff, or school system operations.

Data Governance Plan – a comprehensive set of written documents that outline the roles and responsibilities that constitute the Data Governance Program.

Data Governance Program – The individuals and processes with responsibility for establishing and enforcing policies, administrative regulations, procedures, and guidelines involving data.

3. Policy Statement

The Board of Education of Carroll County and the Carroll County Public Schools acknowledge that data are a critical system resource and commit to managing and using data in support of the system's mission and strategic plan. The system also takes seriously the ethical and legal responsibility to protect the privacy, ensure the security, and govern the use of school system data.

4. Exceptions

There are no exceptions to this policy

5. Guidelines

The Superintendent shall establish a Data Policy Committee to oversee a system-wide Data Governance Program for data throughout the full lifecycle. The Superintendent shall also ensure that administrative regulations and the Data Governance Plan maintain strict compliance with all applicable federal and state laws and regulations.

6. Reports

None

7. Expiration/Review

8. Delegation of Authority

The Superintendent and the Data Policy Committee are responsible for the implementation of this policy.

9. Effective Date

Administrative Regulation

1. Purpose

To establish a Data Governance Program oversight structure and provide guidance for the system Data Governance Plan.

2. Scope

This regulation is applicable to all employees, temporary employees, and contractors of the school system. The regulation must be used to assess the risk to system data associated with conducting business.

This regulation shall provide oversight on the following:

- Data Collection
- Access Control
- Data Disclosure
- Data Breach
- Records Retention
- Data Quality and Integrity
- Transparency
- Non-Disclosure Assurances for Employees
- Acceptable Use Agreements
- Data Security and Privacy Training for Employees

3. Prerequisites

This regulation works in conjunction with numerous other system Policies and Regulations. In the event that related regulations are not clearly aligned with the systems Data Governance Plan, the procedures, standards, and guidelines associated with this regulation shall have predominance.

Associated Policies:

- AF - Student Data Privacy Policy
- EHB - Data Records Retention
- IIAA Selection, Evaluation, and Adoption of Instructional Materials.
- IJND - Telecommunications Policy
- ILB - Test Security and Data Reporting
- JR - Disclosure of Directory Information
- JRB - Protection of Pupil Rights-Surveys, Physical Exams, Marketing Personal Information, and Inspection of Certain Material
- JRC - Family Educational Rights

- JRD - Use of Student's Photograph, Video Image, or Voice for Educational, Informational or Public Relations Purposes

4. Responsibilities

The Data Policy Committee shall be responsible for establishing and sustaining the system Data Governance Program.

The Data Governance Committee is focused on establishing and maintaining system-wide processes and guidelines regarding data collection, quality, availability and use. It does this by:

The Data Governance Coordinator, appointed by the Superintendent, is responsible for leading the overall direction and implementation of the Data Governance Program.

Data Stewards are responsible for implementing data governance policies and standards and maintaining data quality and security.

5. Definitions

Acceptable Use Agreement – The Acceptable Use Agreement is a document that stipulates practices and constraints to which a user must agree before being permitted to access computer systems or data.

Access Controls – Access controls limits entry to information system resources to authorized users, programs, processes, or other systems. Components of an access control system include, for example, physical access, authentication systems, and file encryption.

Breach – A data breach is the intentional or unintentional release of secure information to an untrusted environment.

Breach Notification Plan – A Breach Notification Plan is a systematic, consistent, and documented method for providing stakeholder notification in the event security incident has resulted in a breach. The Breach Notification Plan work in conjunction with the Security Incident Response Plan.

Confidentiality – Confidentiality relates to the management of another individual's personally identifiable information. Confidentiality refers to the obligations of those who receive personal information about an individual to respect the individual's privacy by safeguarding the information

Data Collection – Data collection is the process of gathering and recording information. The process of gathering and recording data results in the creation of a record.

Data Quality and Integrity – Data quality and integrity is the process for ensuring, to the greatest extent possible, that information is accurate, relevant, timely, and complete for the purposes for which it is to be used.

Data Stewards – Data stewards are professional staff who are responsible for implementing data governance policies and standards and maintaining data quality and security. It is the data steward's responsibility to ensure that information is collected, maintained, used, and disseminated in a way that respects privacy, ensures confidentiality and security.

Disclosure – Data disclosure means to permit access to or the release, transfer, or other communication of data by any means. Disclosure can be authorized, such as when a parent or an eligible student gives written consent to share education records with an authorized party. Disclosure can also be unauthorized or inadvertent (accidental). An unauthorized disclosure can happen due to a data breach or a loss. An accidental disclosure can occur when data released in public aggregate reports are unintentionally presented in a manner that allows individual students to be identified.

Non-Disclosure Assurances – Non-Disclosure Assurances for Employees are practices and constraints regarding the disclosure of confidential records. The assurances are intended to minimize the risk of unauthorized or inadvertent disclosure due to human error and misuse of information.

Privacy – Privacy relates to individual autonomy and each person's control over their own information. This includes each person's right to decide when and whether to share personal information, how much information to share, and the circumstances under which that information can be shared

Record – A record is any material created or received by the Board and CCPS or any employee in connection with the transaction of CCPS business. A record includes any form of documented material, including but not limited to paper documents, electronic documents, microfilm, drawings, maps, pictures, and any other documented material in any format in which information is created or maintained

Risk Assessment – Risk assessment is the process of identifying: (1) all assets an organization possesses, (2) all potential threats to those assets, (3) all points of vulnerability to those threats, (4) the probability of potential threats being realized, and (5) the cost estimates of potential losses. Risk assessment enables an organization to at least consider the range of potential threats and vulnerabilities it

faces, and is the first step in effectively securing an information and technology system.

Security – Security means protecting information (in all media) through appropriate administrative, technical, and physical security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Security Incident Response Plan – A Security Incident Response Plan is a systematic, consistent, and documented method of approaching and managing situations that may have a negative impact on the confidentiality, integrity, or availability of system applications or data.

Transparency – Transparency is the obligation to provide notice to the individuals regarding the collection, use, dissemination, and maintenance personal and public information.

6. Procedure

A. The Superintendent shall establish a Data Policy Committee. The committee shall be comprised of seven key members of the Superintendent's Executive Leadership Team (ELT) including the Data Governance Coordinator.

   The Data Policy Committee will:
   - Develop and review Data Governance Policy;
   - Resolve issues identified by the Data Governance Committee;
   - Review data procedures and major data-related decisions proposed by the Data Governance Committee; and
   - Hold program offices accountable for participating in the Data Governance Program and adhering to the Data Governance Policy.

   The Data Policy Committee shall inform and consult with the Data Governance Committee on issues in governance, professional development needs, and concerns of data stewards. As needed, the Data Policy Committee may call upon other CCPS employees to serve in an advisory capacity.

   The Data Policy Committee shall meet, at minimum, biannually.

B. The school system will maintain a Data Governance Committee. The Data Governance Committee with be comprised of the Superintendent's Executive Leadership Team. The Data Governance Committee will:

- Establish, maintain, and enforce standards and procedures for the management of CCPS data.
- Identify individuals to serve as data stewards.
- Support data stewards to resolve data issues and conflicts.
- Hold their program area staff accountable for participating in the Data Governance Program and adhering to the Data Governance Policy.

Individual Data Governance Committee members are designated as the owners of the data in systems and applications that fall under their program areas.

The Data Governance Committee will meet quarterly as an item on regularly scheduled ELT meetings.

C. The Data Governance Coordinator manages the establishment, monitoring, improvement, documentation, and training for the Data Governance Program, as well as for data policies and processes. The coordinator serves as the liaison among data governance groups and members to ensure effective communication. The coordinator also is responsible for identifying program, process, and technological enhancements that will improve data quality and data use and eliminate redundant effort.

D. Data stewards are professional staff who have been identified by the Data Governance Committee. They have responsibility and authority for a given area of data, from collection through use, regardless of where those data reside across the agency. Data Stewards are responsible for:
   - Determining how data are defined, collected, audited, and reported to meet program area requirements and the agency's and external stakeholders' data use needs;
   - Informing how metrics are calculated and how the source system of record is determined for external reporting;
   - Reviewing and approving data releases;
   - Collaborating with other Data Stewards to ensure that the data meet all agency data use needs;
   - Communicating program area needs for data privacy, security, and archiving;
   - Documenting core processes regarding data collection, calculation, and reporting;
   - Ensuring that metadata are documented and maintained;
   - Identifying critical data issues that impede data quality and use;
   - Participating in work groups to identify, propose, and implement resolutions to critical data issues;
   - Tracking federal, state, and other pending legislation or regulations involving data elements in their domains and communicating the potential effects;

- Evaluating and proposing process changes to improve data quality and/or agency efficiency;
- Communicating data governance policies, processes, and decisions to others within the program area.

7. Reports

The CCPS Data Governance Plan shall include procedures, standards, and guidelines that oversee the following lifecycle components:

A. The collection or generation of data
B. Data maintenance: including a data dictionary, inventory, quality and security
C. Data access, breech, use, disclosure, and transparency
D. Data retention and disposal

8. Expiration/Review

9. Effective Date